



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/791,322 | 03/02/2004 | Dmitry Andreev | END920030143 | 1826 |

7590 01/23/2008
Andrew M. Calderon
Greenblum and Bernstein P.L.C.
1950 Roland Clarke Place
Reston, VA 20191

| |
|----------|
| EXAMINER |
|----------|

TABOR, AMARE F

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2139

| | |
|-----------|---------------|
| MAIL DATE | DELIVERY MODE |
|-----------|---------------|

01/23/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/791,322

Applicant(s)

ANDREEV ET AL.

Examiner

Amare Tabor

Art Unit

2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 October 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This correspondence is in response to amendment filed on October 31, 2007.
2. Claims 6, 9, 11, 15, 19 and 21 are amended; Claims 1-5, 7, 8, 10, 12-14, 16-18, 20 and 22 are original.
3. Claims 1-22 are pending.

Response to Arguments

4. Applicant's arguments, see REMARKS, filed on 10/31/2007, with respect to the rejection(s) of claim(s) 9-14 under 35 U.S.C. 101 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn.
5. Applicant's arguments with respect to claims 1-22 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Azuma" (US 2002/0007460 A1) in view of Gregg et al. (US 7,290,288 B2), referred to as "Gregg" hereinafter.

As per Claim 1, Azuma teaches,

A method for authentication in a network, the method comprising: creating a credential string which is derived from a session ID (see Fig. 5-6; where authentication information derived from URL of a web site is disclosed; and for example, abstract; Fig. 3-4; and for example, par. [0015], [0025] to [0031], [0034] and [0037]);

sending (see *Step A7 and B7 in Fig. 3-4; for sending; and for example, par. [0064] and [0096]*) a UserID associated with the session ID and the credential string (see *abstract; Fig. 5; where UserID is associated with URL*);

receiving (see *RECEIVED DATA SAVING MEANS 213 in Fig. 2*) a confirmation request which includes the credential string (see *Fig. 5 and Steps B7-B10 in Fig. 4; and for example, par. [0095] to [0099]*); and sending a response in reply to the confirmation request to validate the credential string to authenticate the UserID (see *Fig. 5 and Steps B11-B13 in Fig. 4; and for example, par. [0100] to [0102]*).

Azuma fails to teach sending a UserID to a software application. However, in the same field of endeavor, Gregg teaches sending a UserID to a software application (see *ACCOUNT HOLDER ADMINISTRATION SOFTWARE 32 in Fig. 1*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to combine the teachings of Azuma and Gregg because both inventions are directed to system and method of controlling the direct access of client user (or computer) to a main server. One having ordinary skill in the art would be motivated to modify the teaching sending credential string to the user authentication proxy by Azuma to sending authentication request to the account holder's administration software as taught by Gregg in order to improve the secure transaction system by a client computer because the administration software is restricted within the organization (see *Fig. 2; and col. 1, line 8 to col. 2, line 13 and col. 4, lines 43-65 of Gregg*).

As per Claim 9, Azuma teaches,

A method for authenticating a user request for a software application, the method comprising: receiving a UserID and a credential string at an authentication proxy server (see *USER AUTHENTICATION PROXY 2 in Fig. 1; and RECEIVED DATA SAVING MEANS 213 in Fig. 2*), the credential string is derived from a session ID (see *Fig. 5-6; where authentication information derived from URL of a web site is disclosed*);

sending a confirmation request from the authentication proxy (see *USER AUTHENTICATION PROXY 2 in Fig. 1*) to a portal (see *WEB SERVER 4 in Fig. 1*), the confirmation request includes the credential string (*request includes information derived from url*);

receiving a response at the authentication proxy for the confirmation request (see *Fig. 5 and Steps B7-B13 in Fig. 4; and for example, par. [0195] to [0102]*); and validating the UserID (see for example, *par. [0064] and [0095]*).

Azuma fails to teach validating using a light weight directory access protocol (LDAP) lookup request and the response. However, Gregg teaches validating using transaction clearing-house server software (see *TRANSACTION CLEARHOUSE SOFTWARE 30 in Fig. 1; Authentication Request 4/Response 5 in Fig. 2; and for example, par. [0037] to [0054]*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to conclude that the clearing-house server software of Gregg validates acting as LDAP of the invention, because the clearing-house software is an SQL database server that registers request and response for all validation requests (see *TRANSACTION CLEARHOUSE DATABASE SERVER 56 in Fig. 4-5; and for example, col. 4, lines 14-42 and col. 6, lines 44-56 and col. 9, lines 3-14 of Gregg*).

As per Claim 15, Azuma teaches,

A system for authenticating a session stored on a computer readable storage medium, comprising computer readable program code (see for example, *par. [0036]*), comprising: an authentication proxy (see *USER AUTHENTICATION PROXY 2 in Fig. 1*) which receives requests to authenticate a UserID and a credential string (see for example, *abstract, par. [0013] to [0015] and [0026] to [0036]*);

a credential string validation component (see *URL and RECEIVED DATA COMPARING MEANS 215 and 216 in Fig. 2*) which receives requests to validate the credential string (see for example, *par. [0037], [0045], [0050] to [0051] and [0100]*).

Azuma fails to teach wherein the credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period. However, Gregg teaches, checking whether the credential string has been previously received for validation within a predetermined time period (see *Step 218-220 in Fig. 18*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention to modify the system Azuma to incorporate Gregg's teaching of checking whether the credential string has been previously received for validation within a predetermined time period because the system prevents unauthorized user from access by periodically re-authenticating (see col. 17, line 55 to col. 18, line 45 of Gregg).

As per Claim 22, Azuma teaches,

A computer program product comprising a computer usable medium having readable program code embodied in the medium, the computer program product including at least one program code to (see for example, *par. [0036]*): create a credential string which is derived from a session ID (see *Fig. 5-6; and for example, abstract; Fig. 3-4; and for example, par. [0015], [0025] to [0031], [0034] and [0037]*);

send a UserID associated with the session ID and the credential string (see *abstract*; *Fig. 5*; *Steps A7 and B7 in Fig. 3-4*; and for example, *par. [0064] and [0096]*);

receive a confirmation request which includes the credential string (see *RECEIVED DATA SAVING MEANS 213 in Fig. 2 and Fig. 5 and Steps B7-B10 in Fig. 4*; and for example, *par. [0095] to [0099]*); and

send a response in reply to the confirmation request to validate the credential string to authenticate the UserID (see *Fig. 5 and Steps B11-B13 in Fig. 4*; and for example, *par. [0100] to [0102]*).

Azuma fails to teach sending a UserID to a software application. However, in the same field of endeavor, Gregg teaches sending a UserID to a software application (see *ACCOUNT HOLDER ADMINISTRATION SOFTWARE 32 in Fig. 1*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention to modify the teaching sending credential string to the user authentication proxy by Azuma to sending authentication request to the account holder's administration software as taught by Gregg in order to improve the secure transaction system by a client computer because the administration software is restricted within the organization (see *Fig. 2*; and col. 1, line 8 to col. 2, line 13 and col. 4, lines 43-65 of Gregg).

As per Claims 2-3, 5, 11-12 and 20, Azuma teaches,

a portal (see *WEB SERVER 4 in Fig. 1*) to create credential string, the portal sends the credential string (see *abstract*; *Fig. 3-4*) and send the UserID to the authentication proxy (see *abstract*; *Fig. 5*).

Azuma fails to teach step of maintaining a password at a portal and not sending the password associated with the UserID to authenticate the UserID; encrypt the credential string by hashing a session ID; and sending to the software application proxy.

However, Gregg teaches maintaining a password at a portal and not sending the password associated with the UserID to authenticate the UserID (*user is authenticated as Log-In Command 2 and Log-In Parameters 3 in Fig. 2*);

encrypt the credential string by hashing a session ID (see *Fig. 11-12*; and for example, col. 13, lines 5-49); and sending to the software application proxy see *ACCOUNT HOLDER ADMINISTRATION SOFTWARE 32 in Fig. 1*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention to modify the teaching sending credential string to the user authentication proxy by Azuma to sending authentication request to the account holder's administration software as taught by Gregg

in order to improve the secure transaction system by a client computer because the administration software is restricted within the organization (see *Fig. 2*; and col. 1, line 8 to col. 2, line 13 and col. 4, lines 43-65 of Gregg).

As per Claims 4, 10 and 16-18, Azuma teaches,

receiving the UserID and credential string (see *RECEIVED DATA SAVING MEANS 213 in Fig. 2 and Fig. 5 and Steps B7-B10 in Fig. 4*; and for example, *par. [0095] to [0099]*);

sending the credential string to the credential string validation component and validating the UserID (see *Fig. 5 and Steps B11-B13 in Fig. 4*; and for example, *par. [0100] to [0102]*); and

returning a successful authentication reply to the software application for establishing a session associated with the session ID, otherwise sending an unsuccessful authentication reply to the software application (see *Steps A13-A15, B4-B6 and B11-13 in Fig. 3-4*).

Azuma fails to teach performing a lightweight directory access protocol (LDAP) lookup; and if the LDAP lookup confirms the UserID and the response validates the credential string; providing a confirmation to the software application if the response is affirmative and the UserID is authenticated by the LDAP lookup.

However, Gregg teaches validating using transaction clearing-house server software (see *TRANSACTION CLEARHOUSE SOFTWARE 30 in Fig. 1; Authentication Request 4/Response 5 in Fig. 2*; and for example, *par. [0037] to [0054]*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to conclude that the clearing-house server software of Gregg validates acting as LDAP of the invention, because the clearing-house software is an SQL database server that registers request and response for all validation requests (see *TRANSACTION CLEARHOUSE DATABASE SERVER 56 in Fig. 4-5*; and for example, col. 4, lines 14-42 and col. 6, lines 44-56 and col. 9, lines 3-14 of Gregg).

As per Claim 6-7, Azuma teaches,

sending the UserID associated with the session ID and the credential string (see *abstract; Fig. 5; Steps A7 and B7 in Fig. 3-4*; and for example, *par. [0064] and [0096]*);

initiating a security breach procedure (see *Steps A13, B4 and B11 in Fig. 3-4; where checking if the user is authorized is performed*); and wherein the security breach procedure causes the termination of any session associated with the UserID (see *Steps A14, B5 and B12 in Fig. 3-4; where an authentication failure message is sent*).

Azuma fails to teach sending the UserID a software application proxy; and checking whether the session ID and the credential string has have been previously received within a predetermined time period.

Ho wever, Gregg teaches sending a software application proxy (see *ACCOUNT HOLDER ADMINISTRATION SOFTWARE 32 in Fig. 1*); and checking whether the session ID and the credential string has have been previously received within a predetermined time period (see *Step 218-220 in Fig. 18*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention to modify the system Azuma to incorporate Gregg's teaching of checking whether the credential string has been previously received for validation within a predetermined time period because the system prevents unauthorized user from access by periodically re-authenticating (see col. 17, line 55 to col. 18, line 45 of Gregg).

As per Claim 8, Azuma teaches,

wherein the receiving step and sending a response step is performed by an authentication proxy (*the receiving and sending response is performed at the USER AUTHENTICATION PROXY; see abstract and Fig. 1; and for example, par. [0014] and [0015]*).

As per Claim 13, Azuma fails to teach,

validating the confirmation request by assuring that the credential string has been received only once for confirmation at the portal, otherwise, if presented more than once, performing at least one of initiating a security breach procedure and notifying a software application proxy.

However, Gregg teaches validating the confirmation request by assuring that the credential string has been received only once for confirmation at the portal (see *Step 214 in Fig. 18; where checking if an active session is in operation is performed*), otherwise, if presented more than once, performing at least one of initiating a security breach procedure and notifying a software application proxy (see *Step 216 in Fig. 18; where unsuccessful session response is sent to the client authenticator*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention to validate confirmation request by checking the existing session is active in order protect the system from unauthorized users logging during the authentication phase.

As per Claim 14, Azuma teaches,

receiving the UserID and a password during a logon to the portal, wherein the UserID is validated in the validating step (*the user terminal 1 sends data to the web server 4 authentication; see Fig. 1; and for example, par. [0025] to [0031]*).

Azuma fails to teach password is maintained at the portal and used to process the confirmation request. However, Gregg teaches maintaining password at the portal and used to process the confirmation request (*user is authenticated as Log-In Command 2 and Log-In Parameters 3 in Fig. 2*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention to maintain the password at the portal in order authenticate the user securely and not to submit the password to unsecured network.

As per Claim 19, Azuma fails to teach teaches,

a software application proxy which receives the UserID and the credential string and detects whether the UserID and the credential string has have been previously received within a predetermined time period.

However, Gregg teaches a software application proxy (see *ACCOUNT HOLDER ADMINISTRATION SOFTWARE 32 in Fig. 1*) receiving the UserID; and checking whether the credential string has have been previously received within a predetermined time period (see *Step 218-220 in Fig. 18*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention to modify the system Azuma to incorporate Gregg's teaching of checking whether the credential string has been previously received for validation within a predetermined time period because the system prevents unauthorized user from access by periodically re-authenticating (see col. 17, line 55 to col. 18, line 45 of Gregg).

As per Claim 21, Azuma teaches,

a portal for accepting a logon by a user and for creating the credential string from an associated session ID (*the user terminal 1 sends data to the web server 4 authentication; see Fig. 1; and for example, par. [0025] to [0031]*).

Azuma fails to teach, a lightweight directory access protocol (LDAP) directory for authenticating the UserIDs and which is accessible by the authentication proxy; and a software application proxy for intercepting the UserID and the credential string sent by the portal for monitoring duplicate occurrences of the UserID and the credential string.

However, Gregg teaches validating using transaction clearing-house server software (see *TRANSACTION CLEARHOUSE SOFTWARE 30 in Fig. 1; Authentication Request 4/Response 5 in Fig. 2; and for example, par. [0037] to [0054]*); and software application proxy for intercepting the UserID and the credential string sent by the portal for monitoring duplicate occurrences of the UserID and the credential string (see *Step 214 and 16 in Fig. 18; where checking if an active session is in operation is performed and unsuccessful session response is sent to the client authenticator*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to conclude that the clearing-house server software of Gregg validates acting as LDAP of the invention, because the clearing-house software is an SQL database server that registers request and response for all validation requests (see *TRANSACTION CLEARHOUSE DATABASE SERVER 56 in Fig. 4-5; and for example, col. 4, lines 14-42 and col. 6, lines 44-56 and col. 9, lines 3-14 of Gregg*).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Application/Control Number:
10/791,322
Art Unit: 2139

Page 10

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
AU 2139


SYED A. ZIA 01/11/2008
PRIMARY EXAMINER